FINANCIAL INFORMATION FORUM

April 26, 2023

By electronic mail to rule-comments@sec.gov

Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090
Attn: Secretary

Re: File Number SR-OCC-2023-003: Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing of Proposed Rule Change by The Options Clearing Corporation Concerning Clearing Member Cybersecurity Obligations

Dear Secretary,

The Financial Information Forum ("FIF")[1] appreciates the opportunity to comment on SR-OCC-2023-003 filed by The Options Clearing Corporation (the "OCC") with the Securities and Exchange Commission (the "Commission")[2] and the Commission's associated Notice of Filing.[3] The filing by the OCC (the "OCC Rule Filing") proposes to "… (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a form containing written representations addressing the incident and attesting to certain security requirements ("Reconnection Attestation") and an associated checklist describing remediation efforts ("Reconnection Checklist" and together, "Reconnection Attestation and Checklist")."[4]

FIF members are concerned about the broad scope of the OCC's proposed definition of Security Incident, the requirement for immediate notification, the proposed authorization for the OCC to

[1] FIF (www.fif.com) was formed in 1996 to provide a centralized source of information on the implementation issues that impact the securities industry across the order lifecycle. Our participants include broker-dealers, exchanges, back office service bureaus, and market data, regulatory reporting and other technology vendors in the securities industry. Through topic-oriented working groups, FIF participants focus on critical issues and productive solutions to technology developments, regulatory initiatives, and other industry changes.
[2] The Options Clearing Corporation, "Proposed rule change by The Options Clearing Corporation concerning Clearing Member cybersecurity obligations," SR-OCC-2023-003 (Mar. 21, 2023), available at https://www.theocc.com/getmedia/54bd8b51-4e9d-4344-bf8b-91a36263eea1/sr_occ_2023_003.pdf ("OCC Rule Filing").
[3] Securities Exchange Act Release No. 97225 (Mar. 30, 2023), 88 FR 20195 (Apr. 5, 2023) ("Notice of Filing").
[4] OCC Rule Filing, at 4.

disconnect a clearing member's access without identifying any threshold conditions that must be satisfied prior to the OCC taking this type of drastic action, the conditions for reconnection, and the lack of clarity as to the intended interaction among the proposed notification, disconnection and reconnection processes. These concerns are discussed below.

FIF members also are concerned that the approach proposed by the OCC in the OCC Rule Filing is inconsistent with regulations and requirements that have been adopted by various financial regulators and other self-regulatory organizations ("SROs") with respect to notification of cybersecurity incidents, including the Commission's Regulation SCI,[5] to which the OCC itself is subject. FIF members recommend that the OCC evaluate these other regulatory and SRO regulations and requirements and propose a rule that is consistent with the approach taken by other regulators and SROs. If the OCC intends to impose requirements that are inconsistent with these other regulations and requirements, the OCC should include in any refiling a written justification for doing so. While FIF members also have certain concerns with these other regulations and requirements, it is important, at a minimum, given the immediacy of the reporting requirement, the multiple reporting requirements to which clearing members are subject, and the complexity of cybersecurity reporting, that the OCC adopt cybersecurity notification requirements that are consistent with the notification requirements imposed by regulators and other SROs.

FIF members also believe there are a number of details in the OCC Rule Filing that require further clarification, as discussed below.

Because the OCC's proposed definition of Security Incident applies to all of a clearing member's systems, the currently proposed definition is inconsistent with the risks identified by the OCC in the OCC Rule Filing, inconsistent with other regulatory and SRO requirements, and potentially beyond the scope of the OCC's authority

The OCC Rule Filing defines a Security Incident as "… a cyber-related disruption or intrusion of the Clearing Member, including, but not limited to, any disruption or degradation of the normal operation of the Clearing Member's systems or any unauthorized entry into the Clearing Member's systems."[6] As currently drafted, a Security Incident could include an incident that would not impact OCC systems. FIF members consider this approach to be overly broad, inconsistent with the risks identified by the OCC in the OCC Rule Filing, inconsistent with the approach taken by other regulators and SROs, and potentially beyond the scope of the OCC's authority.

The OCC provides as follows in the OCC Rule Filing:

> Cybersecurity incidents pose an ongoing risk to OCC, as well as market participants, as an attack on OCC can lead to the loss of data or system integrity, unauthorized disclosure of sensitive information, or an inability to conduct essential clearance and settlement functions. Moreover, as a designated systemically important financial market utility ("SIFMU"), a failure or disruption to OCC could increase the risk of significant

[5] 17 CFR §§242.1000-1007.
[6] OCC Rule Filing, at 44.

> liquidity problems spreading among financial institutions or markets and thereby threaten the stability of the financial system in the United States.[7]

Consistent with the specific risks identified by the OCC, a Security Incident requiring notification to the OCC should be limited to a cybersecurity incident impacting a clearing member's systems that would be reasonably likely to result in "… loss of data or system integrity…" on the OCC's systems, "… unauthorized disclosure of sensitive information …" on the OCC's systems, or "… an inability [for the OCC] to conduct essential clearance and settlement functions."[8]

The Commission's Regulation SCI, to which the OCC (as an SCI entity) is itself subject, requires an SCI entity to notify the Commission of an SCI event.[9] An SCI event is defined as a disruption, compliance issue or intrusion that impacts an SCI system and, in the case of an intrusion, an indirect SCI system.[10] SCI systems are limited to systems that "… with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance."[11] Indirect systems are systems "… that, if breached, would be reasonably likely to pose a security threat to SCI systems."[12] The approach proposed above by FIF members would be consistent with the Commission's approach in Regulation SCI, because it would require notification of a cybersecurity incident that would be reasonably likely to pose a security threat to OCC systems.

As a second example to consider, the National Futures Association (the "NFA"), in NFA Interpretive Notice 9070 on Information Systems Security Programs ("NFA Interpretive Notice 9070"), requires prompt notification to the NFA of "… a cybersecurity incident related to the Member's commodity interest business."[13] The approach proposed above by FIF members would be consistent with the NFA's approach because the scope of reporting would be consistent with the scope of the SRO's area of responsibility.

It is also important to consider whether it would be within the scope of the OCC's authority to request reporting of security incidents that would not impact OCC systems. FIF members request that the OCC provide clarification on this point.

---

[7] Id. at 5-6.
[8] Id. at 5.
[9] 17 CFR §242.1002(b).
[10] 17 CFR §242.1000.
[11] Ibid.
[12] Ibid.
[13] National Futures Association, NFA Interpretive Notice 9070 (NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs), available at file:///C:/Users/meyerson/Downloads/nfa-rules-9-9070.pdf ("NFA Interpretive Notice 9070"), at 3.

The OCC's proposed definition of Security Incident is inconsistent with other regulatory and SRO requirements because the OCC's proposed definition does not require as a condition that a loss or harm has occurred

The OCC's proposed definition of Security Incident does not require as a condition that a loss or harm has occurred. FIF members consider this approach to be overly broad and inconsistent with the approach taken by other regulators and SROs.

As an example of this type of condition, NFA Interpretive Notice 9070 requires prompt notification to the NFA when a cybersecurity incident "… results in: 1) any loss of customer or counterparty funds; 2) any loss of a Member's own capital; or 3) in the Member providing notice to customers or counterparties under state or federal law."[14]

As another example, the Commission's recent cybersecurity risk management rule proposal for broker-dealers and other entities (the "Commission Cyber Proposal") requires notice to the Commission of a "significant cybersecurity incident."[15] The Commission Cyber Proposal defines a significant cybersecurity incident as a cybersecurity incident or group of cybersecurity incidents that either "… significantly disrupts or degrades the ability of the market entity to maintain critical operations" or "… leads to the unauthorized access or use of the information or information systems of the market entity …" where the unauthorized access or use "… results in or is reasonably likely to result in: (A) Substantial harm to the market entity; or (B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity."[16]

As a third example to consider, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System (the "FRB") and the Federal Deposit Insurance Corporation (the "FDIC") have adopted cybersecurity notification requirements that require a banking organization to notify the Office of the Comptroller of the Currency, FRB or FDIC, applicable, if a "notification incident" occurs.[17] As defined, a "notification incident" is "… a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's … Ability to carry out banking operations, activities, or processes … Business lines … or … Operations."[18] A "computer-security incident" is defined as "… an occurrence that results in actual harm to the

[14] Ibid.
[15] Securities Exchange Act Release No. 97142 (Mar. 15, 2023), 88 FR 20212 (Apr. 5, 2023) (Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents) ("Commission Cyber Proposal"), at 20344-20345.
[16] Id. at 20344.
[17] Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, 86 FR 66424 (Nov. 23, 2021) (Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers) ("Computer-Security Notification Requirements for Banking Organizations"), at 66442-66444.
[18] Ibid.

confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[19]

The OCC's proposed definition of Security Incident is inconsistent with other regulatory and SRO requirements because the OCC's proposed definition does not require that a clearing member be aware of the incident

The OCC Rule Filing requires a clearing member to provide immediate written notice of a Security Incident but does not provide a clearing member with the opportunity to evaluate the incident prior to reporting. The OCC Rule Filing also would require a clearing member to report an incident even if the clearing member is not aware of the incident, which is not possible.

The Commission Cyber Proposal requires a firm to "… give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring."[20] The Office of the Comptroller of the Currency, FRB and FDIC regulations require a banking organization to notify the applicable bank regulator of a "notification incident" (see discussion above) "… as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred."[21] The OCC Rule Filing should incorporate into the notice provision a similar condition that only requires reporting when a clearing member has a reasonable basis to conclude that a reportable cybersecurity incident has occurred or determines that a reportable cybersecurity incident has occurred. As discussed above, FIF members also recommend that the definition of security incident be based on the risks enumerated by the OCC in the OCC Rule Filing.

FIF members are concerned with the requirement for immediate notification

While the Commission has proposed in the Commission Cyber Proposal a requirement for immediate notification, FIF members have concerns with this requirement in the Commission Cyber Proposal and the OCC Rule Filing. In particular, a clearing member prior to reporting should have a reasonable opportunity to assess whether a reportable cybersecurity incident has occurred.

FIF members request clarification on the reference to "disruption or degradation of a clearing member's systems" in the proposed definition of Security Incident

The proposed definition of Security Incident in the OCC Rule Filing applies to "… a cyber-related disruption or intrusion of the Clearing Member, including, but not limited to, any disruption or degradation of the normal operation of the Clearing Member's systems …."[22] FIF members request confirmation from the OCC that the reference to disruption or degradation of a clearing member's systems refers to a disruption or degradation of a clearing member's systems that results from a cyber-related disruption or intrusion (i.e., that results from malicious third-party activity). As an example, a

[19] Ibid.
[20] Id. at 20344-20345.
[21] Computer-Security Notification Requirements for Banking Organizations, at 66442-66444.
[22] Id. at 44.

power outage at a data center that does not result from malicious third-party activity should not be a reportable Security Incident. As discussed above, FIF members also recommend that the definition of Security Incident be based on the specific risks identified by the OCC in the OCC Rule Filing.

The OCC Rule Filing should provide an exception when law enforcement directs a member not to disclose

FIF members propose that the OCC provide an exception from the requirement for a clearing member to report a Security Incident for the scenario where a law enforcement authority directs the clearing member not to make such disclosure.

The OCC should provide detail as to the expected content of the immediate notification; this content would need to be limited in scope given the requirement for "immediate" notification

The OCC Rule Filing requires a clearing member to provide immediate written notice of a Security Incident but does not define the content of such immediate notification. FIF members recommend that the OCC provide additional detail as to the required content for an immediate notification. This content would need to be limited in scope given the requirement for "immediate" notification. FIF members note that in the Commission Cyber Proposal the content of an immediate notification is limited with firms required to report additional detail in a written notice that must be submitted within 48 hours after a firm has "… a reasonable basis to conclude that …" a "… significant cybersecurity incident has occurred or is occurring."[23]

FIF members request further clarification on protection of the information reported by clearing members to the OCC

FIF members are concerned that the OCC could become a target for malicious actors if the OCC is in possession of detailed information from clearing members relating to cybersecurity incidents. FIF members request that the OCC include in the OCC Rule Filing additional detail as to the processes that the OCC will have in place to protect the confidentiality of the information relating to cybersecurity incidents that is reported by clearing members to the OCC. FIF members also request that the OCC provide additional detail in the OCC Rule Filing as to the OCC's intended use of the data relating to cybersecurity incidents that is reported by clearing members.

The rule should enumerate threshold conditions that must be satisfied before the OCC could disconnect or modify a clearing member's access

FIF members are concerned that the OCC rule filing authorizes the OCC "… to disconnect access, or to modify the scope and specifications of access, of the Clearing Member to the Corporation's [the OCC's] information and data systems,"[24] but there are no threshold conditions that must be satisfied prior to the OCC taking this type of drastic action. Such an action could have a drastic impact on the disconnected clearing member and the clearing member's customers and counter-parties; there also

[23] OCC Rule Filing, at 20345.
[24] OCC Rule Filing, at 44.

could be a significant market-wide impact resulting from such an action. FIF members recommend that the OCC Rule Filing provide additional detail as to the threshold conditions that would need to occur before the OCC could take the drastic step of disconnecting or limiting a clearing member's access to the OCC's systems.

FIF members request clarification on the relationship between the proposed Security Incident notifications and the proposed disconnection and reconnection process

The OCC Rule Filing provides that a clearing member must, after the clearing member reports a Security Incident to the OCC (and upon request of the OCC), complete and submit a form that describes the Security Incident along with a reconnection attestation and a reconnection checklist. Does this mean that the OCC would disconnect a clearing member every time the clearing member reports a Security Incident? FIF members are opposed to this type of approach. Alternatively, does this mean that the OCC would only request follow-up notification of a Security Incident (after the immediate notification) if the OCC has disconnected the clearing member? To avoid potential confusion, FIF members recommend that the OCC separate the notification process from the disconnection and reconnection process such that a clearing member could provide notification of a Security Incident without a disconnection occurring. As discussed above, any disconnection should be subject to specific conditions and processes that are enumerated in the proposed rule.

FIF members have concerns and questions about the proposed reconnection attestation and checklist

FIF members have the following concerns and questions about the proposed reconnection attestation and checklist:

- The reconnection attestation requires a senior executive of the clearing member to certify that the "… Clearing Member has provided full, complete and accurate information regarding any data or systems of the Corporation that were potentially compromised during the Security Incident, including any potential exposure of credentials used to access the Corporation's systems."[25] The reconnection attestation also requires the executive to certify that the clearing member has communicated to the OCC any failed controls and technical and operational changes implemented by the clearing member.[26] FIF members are concerned that this level of detail could provide a roadmap to malicious actors who could seek to obtain access to the OCC's systems.
- Any disclosure mandate and attestation also should take into account the fact that target firms often have incomplete information about a cybersecurity incident and engage in an investigation process over a period of time.
- FIF members are concerned about the required attestation relating to notifications to other government agencies and third parties. Many clearing members would be subject to numerous governmental and third-party notification requirements in the event of a cybersecurity incident and would make a good faith effort to comply with all reporting obligations within the

[25] Ibid.
[26] Ibid.

mandated reported periods that are applicable for each reporting obligation. FIF members do not understand why the OCC would require an attestation relating to a clearing member's notification to other regulators and third-parties if the clearing member has provided all required notifications to the OCC.

- Any required attestation should be to the knowledge of the attesting executive.
- The information that a firm is required to report in the reconnection checklist is too detailed and could provide a roadmap to malicious actors who could seek to obtain access to the OCC's systems.
- The reconnection checklist appears to be a security incident notification form rather than a checklist for reconnection. The proposed rule should establish a clear process for reconnection, including the process and timing for the OCC to decide on a reconnection request and the process for the OCC to communicate its determination.
- The reconnection checklist requires a clearing member to report whether the disconnection was the result of a cybersecurity-related incident.[27] FIF members do not believe that this checklist item is necessary because the checklist is specific for cybersecurity-related incidents. In addition, the OCC would already be aware of why it disconnected the clearing member.
- FIF members also are concerned that the level of detail that a clearing member is required to report pursuant to the reconnection attestation and checklist could subject the clearing member to material third-party litigation risk.

Given the complexity and detail in the Commission's recent cyber, Regulation SCI and Regulation S-P rule proposals and the overlap between the Commission's proposals and the OCC Rule Filing, the OCC should withdraw the OCC Rule Filing and resubmit the filing after the comment periods for the Commission's proposals have expired

Given the limited time period for comment, this comment letter highlights certain concerns with the proposal in the OCC Rule Filing and does not identify all potential concerns. During the comment period for the OCC Rule Filing, FIF members and other industry participants also are focused on the Commission Cyber Proposal and two other Commission proposals that would require reporting (or changes to current reporting requirements) for certain cybersecurity events: the Commission's rule proposals on Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information[28] and Regulation Systems Compliance and Integrity.[29] Given that FIF members and other market participants are currently focused on these three lengthy and complex Commission rule proposals, and given the overlap in the subject matter of the OCC and Commission rule proposals, FIF members recommend that the OCC withdraw the OCC Rule Filing and resubmit the filing after the comment periods for the Commission rule filings have elapsed. This would be beneficial for three distinct reasons: it would provide industry members and other market participants the opportunity to conduct a proper and comprehensive review of the OCC Rule Filing, including consideration of potential unintended consequences; it would provide the OCC the opportunity to review the Commission's rule filings and ensure consistency between the Commission's rule filings and the OCC Rule Filing; and it would provide

[27] Id. at 45.

[28] Exchange Act Release No. 97141 (Mar. 15, 2023), 88 FR 20616 (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information).

[29] Exchange Act Release No. 97143 (Mar. 15, 2023) (Regulation Systems Compliance and Integrity).

the OCC the opportunity to review the detailed comment letters that will be submitted in response to the Commission's rule filings. While FIF members are currently reviewing the Commission's rule proposals and will have comments on these proposals (including with respect to cyber reporting requirements), the OCC should seek to avoid imposing cyber reporting requirements that are inconsistent with the cyber reporting requirements that the Commission is expected to adopt.

* * * * *

FIF appreciates the opportunity to comment on SR-OCC-2023-003. If you would like clarification on any of the items discussed in this letter or would like to discuss further, please contact me at howard.meyerson@fif.com.

Very truly yours,

/s/ Howard Meyerson

Howard Meyerson
Managing Director, Financial Information Forum